Digital and advanced electronic signature: the security function, especially in electronic commerce

John **Velentzas**[1], ***George*** **Kiriakoulis**[2], ***Georgia*** **Broni**[3], ***Nick*** **Kartalis**[4], ***George*** **Panou**[5], ***George*** **Fragulis**[6]

Abstract

The purpose of Directive 1999/93 / EC on the Community framework for electronic signatures is to facilitate the use of electronic signatures. Digital signatures are incredibly important as they prevent fraud in e-commerce transactions. A legal framework for electronic signatures is established to ensure the smooth functioning of the internal market. This article aims to interpret the European framework for digital signatures.

Member States shall at least ensure that, when issuing a certificate, the certification body is liable for any damage caused to any entity or natural or legal person reasonably based on the certificate:

(a) the accuracy, at the time of issue, of all the information contained in the recognized certificate.

(b) ensure that, at the time of issue of the certificate, the signatories identified on the recognized certificate were the holders of the signature-creation data corresponding to the signature verification data referred to or specified in the certificate;

Member States shall at least ensure that the certified provider is liable for any damage caused to any entity or natural person who reasonably relies on the certificate, unless the certifying provider proves that it did not act negligently.

Member States shall ensure that a certified service provider may indicate in a recognized certificate restrictions on the use of that certificate.

Member States shall ensure that a certification-service-provider may indicate on the recognized certificate the limits on the amount of transactions for which the certificate may be used. For all of the above, the certification service provider is not liable for damages resulting from exceeding these limits.

keywords: **digital signature, advanced electronic signature, Electronic Commerce.**

1. The legislative framework

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 is the Community framework for electronic signatures (Velentzas, 2018:118).

2. Field of application

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. A legal framework for electronic signatures is being established to ensure the smooth running of the internal market.

It does not cover aspects related to the conclusion and validity of contracts or other legal obligations governed by the requirements of the press under national or Community law and does not affect rules and restrictions on the use of documents contained in national or Community law.

3. What is a digital signature

Digital signature is considered to be the electronic equivalent of conventional signature and is a string derived from the combination of binary digits of a message and those of a secret key (Velentzas, 2018:126, Delouka-Igglesi K. 2015:183).

The use of digital signature in a network security system is essential as it provides authentication of the sender, confidentiality and integrity of the message (Velentzas, 2018:129, Igglezakis, 2009:153).

What digital signature allows

Digital signature allows (Velentzas, 2018:127, Delouka-Igglesi K. 2015:185):

- To digitally sign e-mails providing the sender's identification so that no one can be sure who sent the message.
- Encrypt emails, including attachments, so that only selected recipients can read their content
- Have a unique password for accessing computing resources instead of the pair user / password
- To access, complete and "sign" on-line data entry forms, licenses and agreements.

4. Production of the digital signature

The sender applies a hash function to the message to create a message digest message of a predetermined size (Igglezakis, 2009:152).

To create a digital signature, it usually encrypts the message summary and not the message itself (in other words, the encrypted message summary is the sender's digital signature).

[1] John Velentzas, Professor (University of Western Macedonia, ivelentzas@uowm.gr)
[2] George Kiriakoulis, PhD student (University of Western Macedonia, kiriakoulisgeorgios@gmail.com
[3] Georgia Broni, Assistant Professor (University of Western Macedonia, gbroni@uowm.gr)
[4] Nick Kartalis, Professor (University of Western Macedonia, kartalisdn@gmail.com)
[5] George Panou, Assistant Professor (University of Western Macedonia, georgepanou@hotmail.com)
[6] George Fragulis, Professor (University of Western Macedonia, ivelentzas@uowm.gr)

The Sender sends to the recipient the encrypted message summary and the message encrypted or not (Delouka-Igglesi K. 2015:186)

5. Authentication of the digital signature

Recipient B applies, first of all, the same hash function as the Sender (A) in the message received. It thus creates its own version of the correct message summary.

It then decrypts the digital signature received by attaching the message using A.'s public key. This process leads to the reproduction of the message summary created by A.

B now has two summaries at his disposal. He compares them and if they match, he successfully authenticated A's digital signature. If not, there are few possible explanations. Either someone is pretending to be A, or the message has changed since A signed it, or there was a mistake in the broadcast.

6. Definitions

1. "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. "advanced electronic signature" means an electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can maintain under his sole control; and

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

3. "signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;

4. "signature-creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

5. "signature-creation device" means configured software or hardware used to implement the signature-creation data;

6. "secure-signature-creation device" means a signature-creation device which meets the requirements laid down in Annex III;

7. "signature-verification-data" means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;

8. "signature-verification device" means configured software or hardware used to implement the signature-verification-data;

9. "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;

10. "qualified certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;

11. "certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;

12. "electronic-signature product" means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;

13. "voluntary accreditation" means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

7. Market access

1. Member States shall not depend on the provision of pre-approval certification services (Velentzas, 2018:132, Delouka-Igglesi K. 2015:188).

2. Member States may maintain voluntary accreditation mechanisms. All conditions associated with these mechanisms must be objective, transparent, proportionate and not discriminatory. Member States may not limit the number of accredited certification service providers for reasons falling within the scope of this Directive.

3. Each Member State shall ensure the establishment of an appropriate system which makes it possible to monitor the certification service providers established in their territory.

4. Compliance with the safeguards for the creation of a signature to the requirements of Annex III shall be determined by the competent public or private bodies designated by the Member States.

5. The Commission may, in accordance with Article 9, determine and publish reference numbers of generally recognized standards for electronic signature products in the Official Journal of the European Communities.

6. The Member States and the Commission shall work together to promote the development and use of signature verification provisions.

7. Member States may make the use of electronic signatures in the public sector dependent on possible additional requirements. These requirements should not be an obstacle to cross-border services for citizens.

8. Internal market principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive (Velentzas, 2018:133).

2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market (Velentzas, 2018:131).

9. Legal consequences of electronic signatures

Member States shall ensure that advanced electronic signatures (Velentzas, 2018:135, Igglezakis, 2009:151):

a) meet the legal requirements for signature in the same way that a handwritten signature meets the requirements and

b) are accepted as evidence in legal proceedings.

2. Member States shall ensure that legal force is not rejected as evidence in legal proceedings solely on the grounds that:

- is in the form of electronic data, or
- not based on a recognized certificate, or
- not based on a certified certificate issued by an accredited certification provider, or
- not created by a secure signature creation device.

10. Responsibility

1. Member States shall at least ensure that with the issuance of a certificate, the certification service provider is liable for any damage caused to any entity or natural or legal person that is reasonably based on the certificate:

a) as regards the accuracy, at the time of its issuance, of all the information contained in the recognized certificate.

b) to ensure that, at the time of issuance of the certificate, the signatories identified in the recognized certificate were holders of the signature creation data corresponding to the signature verification data referred to or identified in the certificate.

All of the above under the claim that the certification provider has proven that it did not act negligently.

2. Member States shall at least ensure that the issuer who issued the certificate is liable for any damage caused to any entity or natural person justifiably based on the certificate, for failing to record the revocation of the certificate unless the certification provider proves it. that he did not act negligently.

3. Member States shall ensure that a certified service provider may indicate in a recognized certificate restrictions on the use of such certificate. The certification service provider shall not be liable for damages resulting from the use of a recognized certificate that exceeds the restrictions specified therein.

4. Member States shall ensure that a certified service provider may indicate in the recognized certificate limits on the amount of transactions for which the certificate may be used.

The certification provider is not liable for damages arising from exceeding these limits.

11. International aspects

1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if (Velentzas, 2018:137, Delouka-Igglesi K. 2015:191):

a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or

b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or

c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

2. The Commission shall, in order to facilitate cross-border certification services with third countries and to recognize advanced electronic signatures from third countries, formulate proposals for effective implementation of standards and international agreements applicable to certification services.

12. Data protection

1. Member States shall ensure that certification service providers comply with the requisite requirements on the protection of individuals against the processing of personal data.

2. Member States shall ensure that a certification service provider may collect personal data only directly from the person concerned, or with his express consent, and only to the extent necessary for the purposes of issuing and maintaining the certificate. No data may be collected or processed for any other purpose without the express consent of that person.

3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

13.Committee

1. The Commission shall be assisted by an "Electronic-Signature Committee", hereinafter referred to as "the committee".

2. The Committee shall adopt its own rules of procedure.

14. Requirements for qualified certificates

Qualified certificates must contain (Velentzas, 2018:132-133):

a) an indication that the certificate is issued as a qualified certificate;

b) the identification of the certification-service-provider and the State in which it is established;

c) the name of the signatory or a pseudonym, which shall be identified as such;

d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

e) signature-verification data which correspond to signature-creation data under the control of the signatory;

f) an indication of the beginning and end of the period of validity of the certificate;

g) the identity code of the certificate;

h) the advanced electronic signature of the certification-service-provider issuing it;

i) limitations on the scope of use of the certificate, if applicable; and

j) limits on the value of transactions for which the certificate can be used, if applicable.

15. Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must (Velentzas, 2018:133-138):

a) demonstrate the reliability necessary for providing certification services;

b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;

f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in redily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

l) use trustworthy systems to store certificates in a verifiable form so that:

- only authorised persons can make entries and changes,
- information can be checked for authenticity,
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

16. Requirements for secure signature-creation devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:

a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;

b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;

c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

17. Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that (Velentzas, 2018:128):

a) the data used for verifying the signature correspond to the data displayed to the verifier;

b) the signature is reliably verified and the result of that verification is correctly displayed;

c) the verifier can, as necessary, reliably establish the contents of the signed data;

d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;

e) the result of verification and the signatory's identity are correctly displayed;

f) the use of a pseudonym is clearly indicated; and

g) any security-relevant changes can be detected.

Bibliography

Delouka-Igglesi, K. (2015), Legal Issues of Electronic Commerce, (in Greek), 2nd ed., Sakkoulas Publications, Athens / Thessaloniki.

Igglezakis, Yiannis (2009), The legal framework of e-commerce, (in Greek) Sakkoulas Publications, Athens / Thessaloniki.

Igglezakis, Yiannis (2016), The legal regulations for digital signatures. Directive 1999/93 EC and national legislation, (in Greek) Sakkoulas Publications, Athens / Thessaloniki.

Velentzas, John (2020), Business Law, (in Greek), 22nd ed., IuS Publications, Thessaloniki

Velentzas, John (2018), Technology and Innovation Law, (in Greek), 4th ed., IuS Publications, Thessaloniki

Velentzas, John / Kiriakoulis, George / Broni, Georgia / Kartalis, Nick / Panou, George / Charitoudi, Georgia (2020), Digital signature as a security valve in electronic commerce, ICOAE.